Volume 22 | Issue 6 Article 7

1976

Confidentiality of Criminal Records Privacy v. The Public Interest

David Weinstein

CONFIDENTIALITY OF CRIMINAL RECORDS PRIVACY V. THE PUBLIC INTEREST

DAVID WEINSTEIN†

Privacy and Criminal Records

Many people start with the assumption that the collection, retention and disclosure of criminal records, especially records of persons who have been arrested but not convicted, creates a "problem." There is great uncertainty, however, as to what precisely this problem is. One prevalent way of describing it is as a "privacy" problem. Given the difficulty the courts and commentators have had in defining privacy and its legal protection, by simply labeling the problem as one of "privacy" one does not shed much light on it. In reviewing comparatively recent United States Supreme Court decisions, one finds that the "privacy" issue has received rather strikingly different treatment. When governmental interference with important aspects of family life has been contested, the Court has used "privacy" arguments to uphold the freedom of a person to prevent the conception of a child or to terminate a pregnancy once conception has been achieved. The contraception[1] and abortion[2] cases rest on concepts of personal autonomy and freedom from governmental interference in important aspects of personal and family life.

When, however, one examines the Supreme Court's treatment of data collection where "privacy" arguments have been raised, one sees quite a different result. In *Laird v. Tatum*,[3] the Supreme Court held that the plaintiffs were not entitled to challenge, in court, military data collection about their political activities. The substance of the decision is that the mere collection of data does not, in and of itself, give rise to a claim which the courts will recognize. As the plaintiffs and the dissenting opinion explained, the only reason to collect the data is to use it, and, in particular, to use it in a covert way, so that the plaintiffs would never know of its use. Without the right to challenge the data collection, the plaintiffs would, in practice, have no ability to challenge the data use.

---

† Visiting Associate Professor of Law, Temple University; Consultant on Criminal Justice Information Systems to the Pennsylvania Legislature and to the state governments of Connecticut and Massachusetts; Consultant to the Confidentiality Committee of the Philadelphia Regional Planning Council of the Governor's Justice Commission of the Commonwealth of Pennsylvania. B.A., Yale University, 1959; J.D., Harvard University, 1962.

1. Griswold v. Connecticut, 381 U.S. 479 (1965).
2. Roe v. Wade, 410 U.S. 113 (1973).
3. 408 U.S. 1 (1972).

More recently, the Supreme Court in the case of *Paul v. Davis*[4] held that the police could circulate an announcement that the plaintiff was a known shoplifter, even though the prosecution for shoplifting terminated in his favor. The Court said that the United States Constitution does not protect one's reputation, which allegedly was being injured by the police department's activities, and, therefore, the plaintiff had no cause of action under the Federal Civil Rights Act. The thrust of this and other opinions is that the Supreme Court will protect certain kinds of behavior from governmental intrusion, but it will not extend the same protection to information about people.

A recent case, *Whalen v. Roe*,[5] illustrates the striking difference between the Supreme Court's protection of behavior and its comparative lack of concern about the harmful effects of data collection. In that case, the Court upheld a New York statute which mandated reporting of the names of users of certain prescription drugs to a computerized central state data bank. The plaintiffs claimed that protection of their right to confidential medical treatment extended to the collection of data about such treatment. The Court did not agree and upheld the data collection.

Obviously, the Supreme Court can and does make mistakes, but in this instance, the different protection given to behavior and to information about that behavior, reflects a broader problem of bringing data collection and use within the ambit of some "right to privacy." The difficulty lies, in part, in the fact that it is not personal autonomy but rather other interests which persons attempting to restrict government handling of information are seeking to protect.

Information, as the Supreme Court acknowledged, is collected to be used. That use frequently causes harm to people. There is no question but that a person with a criminal record is, on the one hand, denied important benefits and opportunities which are available to other persons, and on the other, is subject to special treatment or disabilities.[6] Persons with criminal records have difficulty in obtaining jobs, occupational licenses and even certain government benefits, such as public housing. The denial of benefits or opportunities is often rationalized on the basis of the criminal record when there is reason to believe that other factors are at work.

---

4. 424 U.S. 692 (1976).
5. 97 S. Ct. 869 (1977).
6. *See, e.g., Hearings on S. 2542, S. 2810, S. 2963 & S. 2964 Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 93d Cong., 2d Sess. at 826 (1974) (Sup. Doc. No. Y4.J89/2:C86/13/974 v.2) (Report of the Comm. to Investigate the Effect of Police Arrest Records on Employment Opportunities in the District of Columbia).

Some courts have held discrimination on the basis of criminal records is equivalent to discrimination on the basis of race because minority group members are arrested more often than others in urban areas.[7] Moreover, persons with criminal records are unusually susceptible to the power of government. Not only do the law enforcement agencies feel freer to deal with them than they would with other citizens, but also persons with criminal records are singled out for special attention. For example, when the call goes out to "round up the usual suspects," those usual suspects are almost always persons with past records. Even if the record is only one of arrest and not conviction, criminal justice agencies as well as others tend to treat the two types of records as equivalent.

Criminal System Use of Data

The criminal justice system has, on the other side of the coin, ample justification for its need for data. Criminal justice agencies need data for management purposes. That is to say, the agencies have a substantial caseload which must be moved through the system in an expeditious and intelligent way. Some of this management data can be of a statistical nature; they show how the bulk of cases is being handled. There is, however, even for management purposes, the need to identify individuals and follow them through the system, so that their particular cases can be handled fairly and swiftly.[8]

Beyond the collection of this relatively innocuous data about the identity of a person and where his or her case is in the system, criminal justice agencies require more detailed and personal information, so that a proper decision can be arrived at in disposing of individual cases.[9] For example, when a person is arrested, certain identifying information is taken down. This information is of a relatively "public" nature. It is the type of information that all of us routinely give out in order to obtain some governmental service or benefit. As a person moves through the criminal justice system, however, the nature and extent of data collection changes. At the bail decisionmaking stage, for example, a great deal of important

7. Gregory v. Litton Systems, Inc., 472 F.2d 631 (9th Cir. 1972); Green v. Missouri Pac. R.R., 523 F.2d 1290 (8th Cir. 1975). The problems presented by employment are discussed in Note, *Employment Discrimination — Title VII — Unlawful to Use Conviction Records as an Absolute Bar to Employment,* 22 WAYNE L. REV. 1251 (1976).

8. *SJIS, State Judicial Information System,* Technical Rep. No. 18, SEARCH Group Inc., Sacramento, Cal. (1976).

9. *See* Final Report, Confidentiality Comm. of the Phila. Regional Planning Council of the Governor's Justice Commission (April, 1976).

personal information is obtained concerning one's family history, financial status, employment, educational status, and the like.[10]

As one moves along through the system, the pace of data collection quickens. Diversion programs, presentence investigations, probation reports, institutional histories, psychological and medical reports, parole agent reports, and the like, begin to accumulate. If an individual seeks or is provided with drug treatment, psychiatric care, employment counseling and other rehabilitative programming, the volume of data multiplies. In the end, criminal justice agencies have compiled almost as complete a dossier about a person as one will find anywhere in this society. When one adds information about past criminal history to this collection and supplements it with investigative and intelligence reports, and then places the whole mass of data in a computer system, the subjects of the data and other persons are rightly concerned.

Data Collection and Computerization

It is not entirely clear how much of this concern is a product of data collection and how much is attributable to computerization. There are three basic positions regarding the effects of automation of data. Some feel that there are no additional risks created by automation. Rather, the process of automation has merely drawn attention to preexisting problems of data collection. A second school of thought argues that automation creates no qualitatively different problems, but rather makes the preexisting problems quantitatively larger. The third position is that automation engenders qualitatively different problems which demand entirely new approaches to their solution, if any there be.

Adherents of the first and second schools of thought acknowledge that conscious action should be taken to deal with problems which either have not been addressed in the past or have grown to proportions which now require additional treatment. The solutions proposed are, however, comparatively conservative ones and focus, mainly, on restricting disclosure of information. If the problem is too much or too rapid dissemination, then a lid can be placed on the rate of dissemination. One can even limit the disclosure of information by "expunging" or "erasing" data; such information, presumably, no longer being available for disclosure.

Those who see the problems of automation in qualitative terms are faced with a more difficult problem. It is not only that certain

10. Much of this information, incidentally, is collected about persons, many of whom will never be convicted of any crime or subjected to any penalty.

inefficiencies in recordkeeping, which formerly provided protection, have been removed, but also that the character of data and the potential for use and abuse have changed. The "qualitativist" position rests on a number of assumptions about power, personality and information.

Among the qualitative changes they note are: new meanings created by agglomeration of previously separate information; social control through total data surveillance; use of new decisionmaking techniques based on rapid manipulation of information; psychological subservience of data subjects to the collectors; undue reliance on the machine with a concommitant dehumanization of life. This list could be multiplied and each item analyzed, in detail, if time permitted. The important point for present purposes is that qualitative effects, if any, result from the computerization of fairly sensitive personal data. In order to combat them, fairly radical solutions may be required. Simple nondisclosure and nonretention policies are not enough.

Data Expungement

Various solutions have been proposed to the problems of criminal justice data collection. The most basic type of solution is to eliminate information. Elimination can be achieved at the outset by simply prohibiting the collection of certain information. With some possible limitations on police surveillance of certain constitutionally protected political and educational activities, there have been few judicially imposed limits on data collection. The attitude of the Supreme Court in *Laird v. Tatum*[11] is typical.

If collection cannot or will not effectively be restricted, then one can move to prevent the storage of data or its retention. This is the thrust of various "expungement" statutes. The purpose of such statutes is to eliminate previously collected information on the occurrence of specified contingencies. A frequently cited contingency is the disposition of a criminal case favorably to the accused. While several state statutes[12] and a few court decisions[13] appear to require expungement or erasure in some circumstances, one finds that their practical effect is somewhat limited. A statute may, for example, require expungement or erasure of certain arrest records or the return of fingerprints and photographs upon an acquittal, but leaves

11. 408 U.S. 1 (1972).

12. *See, e.g.*, MO. ANN. STAT. § 610.100 (Supp. 1977); 1976 N.Y. Laws, ch. 877.

13. United States v. McLeod, 385 F.2d 734, 750 (5th Cir. 1967); Sullivan v. Murphy, 380 F. Supp. 867, 869 (D.D.C. 1974); Eddy v. Moore, 5 Wash. App. 334, 346, 487 P.2d 211, 218 (1971); Irani v. Dist. of Columbia, 272 A.2d 849, 851 (D.C. App. 1971).

untouched and in place all of the other information about the individual which has accumulated in the course of a criminal proceeding.[14] While there seems to be some recent judicial interest in providing an expungement or erasure remedy, examination of the cases indicates that the courts will generally order expungement, in the absence of a statute, when there is a finding that the law enforcement officers had no probable cause, whatsoever, to arrest the accused person.[15] Examination of the facts of these cases indicates that the courts are acting only when there has been a fairly significant abuse of official authority.[16]

The expungement, either by statute or judicial decision, creates new problems. It requires, in effect, that history be rewritten, that events be turned into nonevents, and it attempts to achieve this anomalous result by eliminating a part of the information which has accumulated in the course of a criminal proceeding. There are also real disadvantages to expunging information. For example, the accused person may want evidence of innocence to show to private persons who have the arrest record but not the disposition information. The missing information is also required for proper recordkeeping and accounting. Beyond this, the information may be an important link uncovering a pattern of corruption. Special treatment can be effectively concealed by expunging records.

Restriction of Information

As a practical matter, less drastic solutions are preferred. One common approach is to retain information, after acquittal or other disposition favorable to the accused, but restrict its disclosure. Statutes requiring or authorizing "sealing" of information take this tack. Information is not literally "sealed" but rather is placed in a special status which permits only limited disclosure to particular persons under special circumstances. The information is there, but it is also not there, so to speak. Sealing has some of the advantages of expungement without all the disadvantages. Because of the continued existence of the information it is, however, likely to be less effective in achieving the main goal of removing the detrimental affects of a criminal record.

Another related approach, more applicable to "soft" than "hard" data, is to regulate the form in which information may be kept. If

14. *See, e.g.*, CONN. GEN. STAT. § 54-90 (1960).

15. Commonwealth v. Rose, 370 A.2d 1223 (Pa. Super. Ct. 1977); Commonwealth v. Malone, 366 A.2d 584 (Pa. Super. Ct. 1976); Davidson v. Dill, 180 Colo. 123, 503 P.2d 157 (1972) (dictum).

16. *Cf.* Eddy v. Moore, 5 Wash. App. 334, 487 P.2d 211 (1971), where an acquittal on the merits was sufficient justification for judicially ordered expungement.

automation overcomes the inefficiencies of manual or nonautomated record systems or creates qualitatively different problems, then one can prohibit automation or limit the manner of automation. For example, if criminal justice agencies collect sensitive psychological, financial or family history information, then, in theory, one can simply prohibit computerization of such information.

There are several difficulties with these solutions. First, they assume that it is automation, and not data collection itself, which creates the problem. By focusing on automation, more basic issues of information gathering, governmental decisionmaking and control of individual behavior are avoided. By defining the problem as one of "privacy" which, in turn, is equated with improper disclosure of information, one can postpone, indefinitely, an examination of the appropriate role of government in controlling deviants and deviant behavior — including our own.

A policy of total nonautomation at least has the merit of eliminating a potential source of problems. Some, however, propose a policy of "semiautomation" which recognizes that automation is both useful and harmful. The utility is to be realized and the harm avoided by computerization only if the computer system is dedicated to a single agency's function and is physically separate from other such systems. An array of small computer systems would, in this view, be preferable to a large centralized system. Advocates of this position rest their case on the unstated premise that readily accessible information which can be collected from separate systems to create a personal "dossier" is significantly different from the same information already compiled in a centralized computer system, the access to which is tightly restricted.

Inadequacy of Solutions

With today's computer technology, the practical differences between these approaches to computerization are not too radical. The noncomputerization faction has waged a largely ineffectual struggle. It does not have the organized power and vested self-interest of its opponents. Those with a stake in automation are restrained largely by economics. If the cost of computerization falls, then the remaining barriers will fall with it. So far, all the power is one-sided. Even the attempt to limit the scope of computer systems is unlikely to prevail in the face of technology which allows for easy access by one computer system to data in other systems.

Not only do the proposed solutions have real weaknesses, but it is also not entirely clear that most people want them to work. The thrust of the solutions is the sacrifice of some purported public

benefit to gain some purported private benefit. If the private beneficiaries are actual or alleged criminals, and the public beneficiaries are everyone else, then the perceived public benefit is quite likely to prevail. The general public sees little or no connection between collection and computerization of information about "criminals" and its own "privacy" and related interests. The immediate problem of controlling criminal behavior precludes serious consideration of remote and uncertain consequences. If the computer can be used to "fight crime," then the public is behind it.

Another problem with the proposed solutions is that they address the "nonprivacy" problems only by indirection. If one cannot get a job or a license or a benefit because of an arrest or conviction record, and this is thought to be wrong, then the primary problem is with the decisionmaking process. If decisionmakers consider improper factors or discriminate against people because of criminal records — or use such records as an excuse for other types of discrimination — then the obvious answer is to readjust the decision making process. This would require, however, that meaningful legislation be enacted to eliminate the unintended collateral consequences of an arrest or conviction. This, in turn, would require a definition of which consequences are, in fact, "unintended." Upon closer examination it might well be that most of the consequences of an arrest are, in fact, intended. By focusing on data collection and disclosure, one can avoid hard questions about how we ought to treat people arrested or convicted of crimes. Since the facts of arrest and prosecution are in the public domain and are regularly reported by the press — we would hardly want it any other way — attempts to manipulate the processes of data collection and disclosure without squarely addressing problems of data use ignore certain harsh realities.

If these were the only problems with data confidentiality policies, then we might wholeheartedly endorse them as a useful, if only partial, means of achieving the desired goals. Unfortunately, data confidentiality carries with it the potential for great mischief. As it is, the general public, even its elected representatives, can control governmental bureaucracies only in the most limited way. Public access to important facts is, in theory, essential to the prevention of inefficiency and corruption. Confidentiality policies can become the means by which the inefficient or the corrupt conceal their behavior.

The strongest advocates of open access are the news media. While their interest is, in part, selfish — access to information, especially "inside" information, makes for good copy — they forcefully argue that elimination or concealment of information is an

open invitation to inadequate performance or illegal behavior. The press, however, acknowledges few formal limits on its own access to publicly held information. Self-restraint and enlightened self-interest are considered to be sufficient constraints on journalistic abuse of information.

Conclusion

Compounding the difficulties of defining the problems and planning solutions is the lack of reliable information about their scope and behavioral consequences. The police, on the one hand, allege that law enforcement efforts will fail if adequate information is not readily accessible. In their own view, law enforcement agencies always see a need for more information, with cost as the only major constraint. Yet, we do not know what the consequences would be if the legislature denied police officers access to information about persons arrested but not convicted of crimes. What little we know suggests that the consequences would not be nearly so enormous as they represent.

On the other hand, we don't know what difference it would make if persons arrested, or even convicted, for crimes could fully and effectively conceal that fact. Some people might improve their economic position, but how many and how much is impossible of meaningful prediction. We cannot even begin to estimate, intelligently, what the outcome would be if all criminal justice information were freely available to anyone who wished to see it. The press might be happy but relatively free access in the past hasn't done much to eliminate corruption or improve efficiency. The subjects of the information might be hurt, but perhaps not much more than now.

With so little solid information about the direct — and none at all about the indirect — consequences of data collection, computerization and the solutions to the problems they seem to present, each person must, of necessity, fall back on a set of half-articulated assumptions about governmental power, personal behavior, social control and the like. As long as our ignorance is almost total, we can expect wavering policies and analyses with, perhaps, some minor variations on what we have now.